DISCRETE MATHEMATICS 6 (1973) 333–341. 

# SOME PROPERTIES OF BASIC FAMILIES OF SUBSETS

Thomas H. BRYLAWSKI

*Department of Mathematics, University of North Carolina, Chapel Hill, N. Car. 27514, USA*

Received 4 January 1973

**Abstract.** A *basic system* is a nonempty collection of finite incomparable subsets of a set such that for any two subsets or *bases* in the collection, any element of one basis can be replaced by some element of the other to give another basis in the collection. In a basic system, any subset of one basis can be bijectively exchanged for distinct elements of another; for a finite set, basis complements also have these properties; and certain conditions will guarantee that two such systems on the same set will contain a common basis. All proofs are new, elementary, and set-theoretic. In addition, they suggest efficient algorithmic procedures whose efficiencies are calculated.

## 1. Introduction

Many examples can be found in mathematics of a set $S$ together with a certain nonempty family $\mathcal{B}$ of incomparable subsets of $S$ which satisfy the set-theoretic property of the "basis exchange" axiom of combinatorial pregeometries (see Definition 1). These include:

(1) Maximal independent sets of (torsion-free) elements in a Noetherian module.

(2) Bases of a finite dimensional vector space over a division ring.

(3) Vertex spanning, circuit-free subsets of edges of a finite graph.

(4) Maximal supports of partial bijections (matchings) dominated by a relation $R \subseteq S \times X$ in which either $S$ or $X$ is finite.

(5) Maximal collections of subsets of a finite set with a system of distinct representatives as well as maximal sets of rows of a (0–1)-matrix which dominate a square submatrix with a nonzero permanent.

(6) Transcendence bases relative to a ground field $k$ of an extension field $K$ of finite transcendence degree (i.e., maximal sets of algebraically independent elements over $k$ of elements $S$ in $K$ transcendental over $k$).

Properties, apparently stronger than basis exchange, have appeared in the literature for such a family $\mathcal{B}$. Usually, these results have been phrased in the language of combinatorial geometries (matroids) with some familiarity with the subject of geometries needed to follow their proofs.

We mention some of the more striking of these results and outfit them with new and purely set-theoretic proofs. Although no knowledge of the theorems and vocabulary of combinatorial geometries is needed to follow the following arguments the reader may be motivated to find out more about the area in which these results were first conjectured and studied (e.g. [2, 4, 5]).

The main results of the paper can then be reinterpreted for each of the preceding examples. For example, Proposition 2 applied to (2) states that the domains of maximal partial bijections dominated by a relation have a common cardinality (a result proved most directly by the "augmenting path theorem"). Proposition 5 applied to (3) states that minimal subsets of edges which meet every circuit of a finite graph have properties similar to bases (thereby suggesting the notion of the dual of a planar graph). Proposition 6 applied to (6) suggests that if $A = \alpha_1, ..., \alpha_n$ and $B = \beta_1, ..., \beta_n$ are two transcendence bases of an extension field $K$ relative to a ground field $k$, then for some permutation $\sigma \in S_n$, $(A - \alpha_i) \cup \beta_{\sigma(i)}$ are algebraically independent subsets over $k$ for $i \in [1, n]$. Corollary 8, when applied to (5), gives us the special case that if a set $S$ contains $2k + 1$ (or $2k$) elements and if there are two families $\mathcal{F}_1$ and $\mathcal{F}_2$ each consisting of $k$ subsets of $S$ such that in $S$ there are two disjoint systems of distinct representatives for each family of subsets $\mathcal{F}_1$ and $\mathcal{F}_2$, then $S$ contains a system of distinct representatives common to $\mathcal{F}_1$ and $\mathcal{F}_2$. Finally, Proposition 9 in the context of (3) states that given any two spanning trees of finite connected graph and a subset of edges in one, there is a subset of edges in the other such that if the subsets are exchanged between the two trees, two new spanning trees result.

Our proofs are all constructive and for these cases, algorithms are implicitly given. We then estimate upper bounds on the number of steps needed for the algorithms. An example of our methods then determines that, in order to find a subset of column vectors $Y'$ of a non-singular $100 \times 100$ matrix $Y$ to symmetrically exchange with 20 column vectors $X'$ of a non-singular matrix $X$, one needs to compute at most $5 \times 10^{10}$

determinants. On the other hand, finding this subset by the classical method of the Laplace expansion theorem:

$$\det M(X) \det M(Y) =$$

$$= \sum_{Y' \subseteq Y} \pm \det M((X - X') \cup Y') \det M((Y - Y') \cup X')$$

involves the computation of over $10^{21}$ determinants.

## 2. The main results

**Definition 1.** A nonempty family $\mathcal{B}$ of incomparable finite subsets of a set $S$ will be called a *basic system* if for all $B, B' \in \mathcal{B}$ and all $x \in B$, there is a $y \in B'$ such that $(B - x) \cup y \in \mathcal{B}$. The members of $\mathcal{B}$ are called *bases* and we say that $x$ can be *exchanged for* $y$. Note that by incomparability, we may assume that if $x \in B - B'$, then $y \in B' - B$.

**Proposition 2.** *All bases in a basic system are equicardinal. We call this common cardinality the* dimension $\dim(\mathcal{B})$ *of the system.*

**Proof.** Given bases $B$ and $B_1$, we may inductively exchange an element $x_i \in B_i - B$ for an element $y_i \in B - B_i$, obtaining a new basis $B_{i+1} = (B_i - x_i) \cup y_i$ which is equicardinal with $B_i$ but with decreasing symmetric difference with $B$. We may proceed until $B_n - B$ is empty in which case by incomparability $B_n = B$ and $|B_1| = |B_n| = |B|$.

The proof of the following proposition is immediate.

**Proposition 3.** *Given subsets $S_1$ and $S_2$ of $S$, the family $\mathcal{B}'$ of all bases of $\mathcal{B}$ which contain $S_1$ and are disjoint from $S_2$ if nonempty is also a basic system. Hence the family $\mathcal{B}'' = \{B - S_1 : B \in \mathcal{B}'\} = \{B - S_1 : B \in \mathcal{B}, S - S_2 \supseteq B \supseteq S_1\}$ denoted $\mathcal{B}/S_1 - S_2$ is a basic system of the set $S - (S_1 \cup S_2)$ of dimension* $\dim(\mathcal{B}) - |S_1|$.

**Proposition 4** (Symmetric exchange axiom). *If $\mathcal{B}$ is a basic system with bases $B$ and $B'$, then for all $x \in B$, there exists $y \in B'$ such that $(B - x) \cup y$ and $(B' - y) \cup x$ are both bases. We say $x$ can be* exchanged *with $y$.*

**Proof.** We use induction on $\dim(\mathcal{B})$ noting that the result is trivial for dimension one (and zero). Assume the proposition holds for dimension $n-1$ and let $\dim(\mathcal{B}) = n$. Let $X$ and $Y$ be two bases of $\mathcal{B}$ with $x \in X$. We will find $y \in Y$ which can be exchanged with $x$. Assume $y_1$ can be exchanged for $x$ giving

$$B_1 = (X - x) \cup y_1 .$$

Now exchange $y_1 \in Y$ for an element in $X$. If it can be exchanged for $x$, we are done, so assume it can be exchanged for $x'$. Then we have

$$B_2 = (Y - y_1) \cup x' .$$

But $B_2' = B_2 - x' = Y - y_1$ and $X' = X - x'$ are both bases of the basic system $\mathcal{B}/x'$ of dimension $n - 1$, so by the induction hypothesis we may symmetrically exchange $x \in X'$ with something, say $y_2$, in $B_2'$. $X'$ then becomes $B_3' = (X - x - x') \cup y_2$ and $B_2'$ becomes $B_4' = x \cup (Y - y_1 - y_2)$. Hence in $\mathcal{B}$ we have bases

$$B_3 = (X - x) \cup y_2 ,$$
$$B_4 = x \cup x' \cup (Y - y_1 - y_2) .$$

Now exchange $x' \in B_4$ for some element $y'$ in $Y$. But since $x' \in B_4 - Y$, $y' \in Y - B_4 = \{y_1, y_2\}$. Thus either

$$B_5 = x \cup (Y - y_1)$$

or

$$B_6 = x \cup (Y - y_2)$$

are in $\mathcal{B}$. But $B_5$ along with $B_1$ proves the proposition with $y = y_1$ and $B_6$ along with $B_3$ proves the proposition with $y = y_2$.

**Proposition 5** (Dual basis axiom). *If $S$ is finite, then the system of complements of $\widetilde{\mathcal{B}}$, $\mathcal{B} = \{S - B: B \in \mathcal{B}\}$ is a basic system occasionally called the* dual *or* orthogonal *basic system of $\mathcal{B}$. We have* $\dim(\widetilde{\mathcal{B}}) = |S| - \dim(\mathcal{B})$.

**Proof.** Given $B, B' \in \widetilde{\mathcal{B}}$ and $x \in B$, then either $x \in B'$ in which case exchange is trivial, or $x \in S - B' \in \mathfrak{B}$ and it can be exchanged in $\mathfrak{B}$ with $y \in (S - B) - (S - B') = B' - B$ to give $B'' = ((S - B) - y) \cup x$ which is a basis of $\mathfrak{B}$. Hence $S - B'' = (B - x) \cup y$ is in $\widetilde{\mathfrak{B}}$, where $y \in B'$, and the exchange axiom is satisfied.

The following proposition was discovered by Brualdi as a generalization of a theorem about transversals [1]. His original proof was considerably longer and nonconstructive. He also showed by counterexample that the proposition cannot be strengthened to guarantee a bijection for symmetric exchanges.

**Proposition 6** (Bijective exchange axiom). *Given two bases $B$ and $B'$ in $\mathfrak{B}$, there is a bijection $f: B \to B'$ such that for all $x \in B$, $(B - x) \cup f(x)$ is in $\mathfrak{B}$.*

**Proof.** Again we use induction on $\dim(\mathfrak{B}) = n$ noting that for $n = 1$, the result is trivial. Now assume $\bar{x} \in B$ can be symmetrically exchanged with $y \in B'$. Then $(B'-y) \cup \bar{x} \in \mathfrak{B}$, so that both $\bar{B} = B - \bar{x}$ and $\bar{B}' = B' - y$ are in $\mathfrak{B}/\bar{x}$ (a basic system of dimension $n-1$). Hence by induction, we may find a bijection $f': \bar{B} \to \bar{B}'$ such that $(\bar{B} - x) \cup f'(x)$ is in $\mathfrak{B}/\bar{x}$ for all $x \in \bar{B}$, where $f'(x) \in \bar{B}' = B' - y$. But then $(B - x) \cup f'(x)$ is in $\mathfrak{B}$ for all $x \in B - \bar{x}$; and defining $f(x) = f'(x)$ for $x \neq \bar{x}$ and $f(\bar{x}) = y$, gives the required bijection.

**Proposition 7.** *Let $S$ be a set with $2k + 1$ elements. If $\mathfrak{B}_1$ is a basic system on $S$ of dimension $k + 1$ with $B_1, B_1' \in \mathfrak{B}_1$ such that $B_1 \cup B_1' = S$, and if $\mathfrak{B}_2$ is a basic system on $S$ of dimension $k$ with $B_2, B_2' \in \mathfrak{B}_2$ such that $B_2 \cap B_2' = \emptyset$, then there are bases $\bar{B}_1 \in \mathfrak{B}_1$ and $\bar{B}_2 \in \mathfrak{B}_2$ such that $\bar{B}_1$ and $\bar{B}_2$ partition $S$ (i.e. $\bar{B}_1 = S - \bar{B}_2$).*

**Proof.** We prove this by induction on $k$ noting that the result is trivial for $k = 0$. Assume we have proved the proposition for $k = n - 1$. Let $S = 2n + 1$ and let $B_1, B_1', B_2$ and $B_2'$ be as specified above. Then $|B_1 \cap B_1'| = 1$ and $|B_2 \cup B_2'| = 2n$. Assume $B_1 \cap B_1' = x$ and $S - (B_2 \cup B_2') = y$.

*Case 1*: $x \neq y$. Since $B_1 \cup B_1' = S$, we may assume $y \in B_1 - B_1'$. Exchange $y$ with some element, say $z$, from $B_1' - B_1$ to get

$$\hat{B}_1' = (B_1' - z) \cup y \quad \text{in } \mathfrak{B}_1.$$

Then $B_1 \cap \hat{B}'_1 = \{x, y\}$ and $S - (B_1 \cup \hat{B}'_1) = z$. Since $S - (B_2 \cup B'_2) = y \neq x$, we may assume $x \in B'_2 - B_2$. Exchange $x$ for some element, say $w$, from $B_2 - B'_2$ to get

$$\hat{B}'_2 = (B'_2 - x) \cup w \quad \text{in } B_2.$$

Then $B_2 \cap \hat{B}'_2 = w$ and $S - (B_2 \cup \hat{B}'_2) = \{x, y\}$. $B_1 - \{x, y\}$ and $\hat{B}'_1 - \{x, y\}$ are disjoint dimension $n - 1$ bases of the system $\mathcal{B}'_2 = \mathcal{B}_1 / \{x, y\}$ on the $2(n - 1) + 1$ set $S - \{x, y\}$; and $B_2$ and $\hat{B}'_2$ are dimension $n$ bases of $\mathcal{B}'_1 = \mathcal{B}_2 - \{x, y\}$ whose union is $S - \{x, y\}$, so by induction there exist bases $\bar{B}'_1 \in \mathcal{B}'_1$ and $\bar{B}'_2 \in \mathcal{B}'_2$ which are disjoint and whose union is $S - \{x, y\}$.

Then if we let $\bar{B}_1 = \bar{B}'_2 \cup \{x, y\}$ and $\bar{B}_2 = \bar{B}'_1$, we have that $\bar{B}_1 \in \mathcal{B}_1$, $\bar{B}_2 \in \mathcal{B}_2$, and $\bar{B}_1$ and $\bar{B}_2$ partition $S$ as required.

*Case 2*: $x = y$. Let $y'$ be any element of $S$ distinct from $x$ and proceed as in Case 1, but make both exchanges with $y'$ (instead of $y$ and $x$ respectively) to find two $\mathcal{B}_1$ bases containing $x$ and $y'$ and two $\mathcal{B}_2$ bases containing neither $x$ nor $y'$. We can then make the same arguments finding a basis $\bar{B}'_2$ in the system $\mathcal{B}'_2 = \mathcal{B}_1 / \{x, y'\}$ and a basis $\bar{B}'_1$ in $\mathcal{B}'_1 = \mathcal{B}_2 - \{x, y'\}$ such that $\bar{B}'_1$ and $\bar{B}'_2$ partition $S - \{x, y'\}$, so that $\bar{B}_1 = \bar{B}'_2 \cup \{x, y'\} \in \mathcal{B}_1$ and $\bar{B}_2 = \bar{B}'_1 \in \mathcal{B}_2$ partition $S$.

**Corollary 8** (Common basis axiom). *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are two basic systems of dimension $k$ on a set with $2k$ or $2k + 1$ elements and if each contains two disjoint bases, then they contain a common basis.*

**Proof.** Adjoining an element to the set if necessary to give it cardinality $2k + 1$, we then consider $\tilde{\mathcal{B}}_1$ and $\mathcal{B}_2$ which satisfy the conditions for Proposition 7, so that both $\mathcal{B}_1$ and $\mathcal{B}_2$ contain the common basis $\bar{B}_2 = S - \bar{B}_1$.

The following proposition was first proved by Greene [3] and proved independently by the author. It was conjectured by Professor G.-C. Rota based on results in classical invariant theory. There are two advantages of the following proof: It does not rely on the theory and notation of combinatorial geometries. Further, a careful reading of the steps involved shows that the exchange may be effected "one element at a time", thereby leading to an algorithm which grows linearly with the dimension of the basic system.

We prove this axiom by constructing a sequence of intermediate bases which we display as a subset of $X$ followed by a subset of $Y$.

**Proposition 9 (Symmetric subset exchange axiom).** *If $X$ and $Y$ are bases of $\mathcal{B}$ and $X'$ is a subset of $X$, then there exists a subset $\bar{Y} \subseteq Y$ such that $(X - X') \cup \bar{Y}$ and $(Y - \bar{Y}) \cup X'$ are both in $\mathcal{B}$.*

**Proof.** Considering $\mathcal{B} - (S - (X \cup Y))$, we may assume $S = X \cup Y$. We use induction on $k = |X'|$ noting that the result is Proposition 4 for $k = 1$. Now assume the proposition holds for all $k < n$, and let $|X'| = n$ with $x \in X'$. By induction, we may exchange $X' - x \subseteq X$ (symmetrically) with some subset $Y'$ of $Y$ to get bases

$$B_1 = X - (X' - x) \cup Y',$$
$$B_2 = (X' - x) \cup (Y - Y').$$

Now exchange $x$ in $B_1$ $(-Y)$ with some element $y \in Y - Y'$ in $Y$ $(-B_1)$. This gives bases

$$B_3 = (X - X') \cup (Y' \cup y),$$
$$B_4 = x \cup (Y - y).$$

Now exchange the $n - 1$ subset $X' - x$ in $X$ symmetrically with some subset $Y'' \subseteq Y - y$ in $B_4$ to obtain bases

$$B_5 = (X - X') \cup x \cup Y'',$$
$$B_6 = X' \cup (Y - (Y'' \cup y)), \quad \text{where } y \in Y - (Y' \cup Y'').$$

Since $y \notin Y'$, we have $Y' - Y'' \subseteq B_6 - B_2$ and so exchanging $Y' - Y''$ in $B_6$ for some subset of $B_2$ $(-B_6)$, we note that since $X' \subseteq B_6$, we can only get a subset of $Y - Y'$ from $B_2$ in which case $B_6$ will become a basis $B_7$ containing $X'$ and a subset of $Y - Y'$. Since $|X'| = n$ and $|Y'| = n - 1$, this subset must be all of $Y - Y'$ except one element $y'$. But $Y - (Y' \cup Y'' \cup y)$ is already in $B_6$ and is not exchanged out, so that $y'$ can only be in $Y'' \cup y$. Hence

$$B_7 = X' \cup (Y - (Y' \cup y')), \quad \text{where } y' \in (Y - Y') \cap (Y'' \cup y).$$

Exchange $x \in B_5$ $(-B_3)$ for some element in $B_3$, to get $B_8$. Since $(X - X') \subseteq B_5$, we must get some $y'' \in Y' \cup y$ from $B_3$. But since $Y''$ is a subset of $B_5$, $y''$ is not in $Y''$. Thus

$$B_8 = (X - X') \cup Y'' \cup y'' , \qquad \text{where } y'' \in (Y' - Y'') \cup y .$$

Now let

$$\mathcal{B}_1 = \mathcal{B}/((X - X') \cup (Y' \cap Y'')) - (X' \cup (Y - (Y' \cup Y'' \cup y))).$$

This is on the set $S' = (Y'' - Y') \cup (Y' - Y'') \cup y$. The family $\mathcal{B}_1$ contains the bases

$$B_8' = B_8 - (X - X') - (Y' \cap Y'') = (Y'' - Y') \cup y'' ,$$
$$B_3' = B_3 - (X - X') - (Y' \cap Y'') = (Y' - Y'') \cup y .$$

Then $B_8' \cap B_3' = y''$ and $B_8' \cup B_3' = S'$. Let

$$\mathcal{B}_2 = \mathcal{B}/(X' \cup (Y - (Y' \cup Y'' \cup y))) - ((X - X') \cup (Y' \cap Y''))$$

also on the set $S'$ with the bases

$$B_6' = B_6 - X' - (Y - (Y' \cup Y'' \cup y)) = Y' - Y'' ,$$
$$B_7' = B_7 - X' - (Y - (Y' \cup Y'' \cup y)) = ((Y'' - Y') \cup y) - y' ,$$

so that $B_6' \cap B_7' = \emptyset$ and $B_6' \cup B_7' = S' - y'$. Now apply Proposition 7 to get disjoint bases $\overline{B}_1' \in \mathcal{B}_1$ and $\overline{B}_2' \in \mathcal{B}_2$. Hence $\mathcal{B}$ contains the disjoint bases

$$\overline{B}_1 = \overline{B}_1' \cup (X - X') \cup (Y' \cap Y'') ,$$
$$\overline{B}_2 = \overline{B}_2' \cup X' \cup (Y - (Y' \cup Y'' \cup y)) ,$$

with $\overline{B}_1 \cap X = X - X'$ and $\overline{B}_2 \cap X = X'$. Letting $\overline{Y} = \overline{B}_1 \cap Y$, we are finished.

## 3. Algorithmic efficiency

The main advantage of the above proofs is that they lend themselves readily to the construction of algorithms for performing the appropriate exchanges. We emphasize this fact by calculating the efficiency of the above implied algorithms.

Assuming an efficient method for checking whether a given subset is a basis (e.g. lexicographic ordering of elements or computing determinants), we note that if $\dim(\mathcal{B}) = n$, making an exchange takes at most $n$ checks while a symmetric exchange takes $2n$. Hence Proposition 6 shows that the exchange bijection takes at most $2n + 2(n-1) + ... = n^2 + n$ checks which is considerably less than the $n(n!)$ checks one might naively expect.

For Proposition 7, we note that at worst we need $k + 1$ checks for $\mathcal{B}_1$ and $k$ for $\mathcal{B}_2$ to get from case $k$ to $k - 1$. Hence $(k+1)^2$ checks are needed in all.

For Proposition 9, if $f(n, k)$ is the maximum number of checks needed to exchange a $k$-subset of an $n$-basis, we may assume $k \leq \frac{1}{2}n$ (otherwise exchange the complement). Following through the proof we observe $B_1$ and $B_2$ will take $f(n, k-1)$ checks, $B_3$ and $B_4$ will take at most $2(n-k+1)$, $B_5$ and $B_6$ will take $f(n-1, k-1)$, $B_7$ will take at most $n-k+1$, while $B_8$ at most $k$. $|S'| \leq 2k - 1$ and finishing up by Proposition 7 with less than $4k^2$ checks we get

$$f(n, k) < f(n, k-1) + f(n-1, k-1) + 3n + 4k^2$$

and hence $f(n, k) < 2^k nk^2$, which is considerably less than the naive bound of $2\binom{n}{k}$.

## References

[1] R.A. Brualdi, Comments on bases in dependence structures, Bull. Austral. Math. Soc. 1 (1969) 161–167.

[2] H. Crapo and G.-C. Rota, Combinatorial geometries (M.I.T Press, Cambridge, Mass., 1970) preliminary edition.

[3] C. Greene, A multiple exchange property for bases, to appear.

[4] W.T. Tutte, Introduction to the theory of matroids (American Elsevier, New York, 1970).

[5] H. Whitney, On the abstract properties of linear dependence, Am. J. Math. 57 (1935) 509–533.